The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

08/13/2013

SUBJECT:

Vulnerability in Microsoft Unicode Scripts Processor Could Allow Remote Code Execution (MS13-060)

OVERVIEW:

A vulnerability has been discovered in the Unicode Scripts Processor that could allow a remote attacker to take complete control of a vulnerable system. The Unicode Script Processor (USP10.DLL), also known as Uniscribe, is a collection of APIs that enables a text layout client to format complex scripts.

This vulnerability can be exploited if a user visits a specially crafted webpage or opens a specially crafted e-mail attachment. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in the Microsoft Unicode Scripts Processor that could allow a remote attacker to take complete control of a vulnerable system. The vulnerability is caused when the Unicode Scripts Processor, included in affected versions of Microsoft Windows, incorrectly parses specific font types in a way that corrupts memory and allows for arbitrary code to be executed. The Unicode Script Processor (USP10.DLL), also known as Uniscribe, is a collection of APIs that enables a text layout client to format complex scripts. The Unicode Scripts Processor is a Windows component which may be used by both Microsoft software and third-party applications. Successful exploitation could allow an attacker to

gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/security/bulletin/ms13-060

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3181

SecurityFocus:

http://www.securityfocus.com/bid/61697